IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of)

KAMINAGA et al.)

Application Number: 09/935,654)

Filed: August 24, 2001)

For: TAMPER-RESISTANT MODULAR MULTIPLICATION METHOD)

Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT

Sir:

Pursuant to 37 C.F.R. §§ 1.56 and 1.97, this Information Disclosure Statement is submitted in the above-identified patent application. A listing of documents to be published on the face of any patent granted from this application is submitted herewith on Form PTO-1449. Any other documents or information submitted for consideration by the Examiner are listed in this paper. A copy of each U.S. and foreign patent, or each publication or portion thereof listed or herein identified, is submitted herewith.

CERTIFICATION

This Information Disclosure Statement is submitted prior to the mailing date of the first Office Action on the merits in the above-identified application. Accordingly, no fee is due or payable at this time.

Please charge any additional fees or credit any overpayments in connection with this paper to Deposit Account No. 08-1480.

Stanley P. Fisher
Registration Number 24,344

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

January 8, 2002

Form PTO 1449 U.S. Department of Commerce Patent and Trademark Office Information Disclosure Statement by Applicant	ATTY. DOCKET NUMBER Nitt-0028	SERIAL NUMBER To be assigned
	APPLICANT KAMINAGA et al.	
	FILING DATE Concurrently herewith	GROUP

U.S. Patent Documents

Examiner Initial		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE

Foreign Patent Documents

Examiner Initial		DOCUMENT NUMBER	FILING DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION	
							YES	NO
		EP 0 801 345 A1	4/2/97	EPO			X	
		EP 1 006 492 A1	11/25/99	EPO			X	
		EP 1 134 653 A2	3/15/01	EPO			X	

Other Documents (Including Author, Title, Date Pertinent Pages, Etc.)

		Paul C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems, Advances in Cryptology - Crypto 96, 16th Annual International Cryptology Conference, Aug 18-22, 1996, Vol. Conf. 16, pp. 104-113.
		Thomas S. Messerges, Ezzy A. Dabbish, Robert H. Sloan, "Power Analysis Attacks of Modular Exponentiation on Smartcards", Cryptographic Hardware and Embedded Systems, International workshop August 1999, pp 144-157

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant